CASPERTECH TRUST IN COMMUNICATIONS

Cryptech® Linux Manual

This quick start guide will help you to start making and receiving encrypted phone calls in few easy steps and learn how to manage your security functions. After this quick set up you will be able to perform the basic operations. However we recommend you to read carefully the full documentation that comes with the device.

⚠ **To be able to make encrypted phone calls, make sure that the CSD DATA/FAX GSM channel of your SIM card is enabled (please check this feature with your mobile service provider). The data channel activation is usually free of charge, and you will often get an additional data and fax number.**

1. Begin using Cryptech

When you turn on the device for first time, Cryptech will ask you to initialize it inserting a "User Password" two times for confirmation. The User Password will be used for authentication every time you will switch on the phone, so that nobody can use the phone except you.

2. Initialize Cryptech with your User Password

The User Password controls the access to Cryptech application and to the storage area of the cryptographic keys which make your conversations secure. Once your User Password has been set, you will be able to insert and manage your own cryptographic keys .
To change your User Password, select: Menu>(4)settings>(1)general>(1)security>(2)user password.
Chose a password, type it twice in the fields where it is required and click "Done".

⚠ **Do not forget your authentication user password because without it Cryptech can't be launched and you will need to contact Casper Technology for software replacement/restore**

After inserting your User Password the black screen with the CRYPTECH logo will appear, showing the mobile operator you are connected to and the time. You can set the correct date and time going to: menu>(4)settings>(1)general>(3)date and time

3. Dialers

For ENCRYPTED CALLS the phone shows a black dialer with Cryptech logo in red.
For CLEAR CALLS the dialer is white and there is no Cryptech logo.
The phone by default allows only encrypted calls, and we highly recommend to use it only in this way.
You can change settings and use it also for sending and receiving clear call and sms going to :
Menu>(7) Enable standard call

4. Clear call

By default clear call are disabled for security reasons. But if you need to use the phone also for normal call and sms you can go to: Menu>(7)enable standard call. To go to the Clear calls dialer you simply press the button with the symbol of a note which is just under the green button. To switch to Crypto mode press the same button and enter your User Password to access the Crypto mode. When you receive a call the phone automatically propose you the right interface: the white dialer for clear calls and the black dialer with Cryptech logo for crypto calls. Switching between the two modes, you have always to authenticate yourself with user password passing from clear to crypto until you change it going into:
menu>(4)settings>(1)general>(1)security>(4)Auth crypto dialer

5. Make an encrypted call

Once you have the Cryptech dialer on your display, to make an encrypted call you can either dial the number directly on the keypad, or you can import the telephone number from your Contact List (select "Contacts"). Then press the green "Call" button (1): after a synchronization phase, the call will start. During synchronization you'll see a bar showing the progress of data exchange of the connection protocol. At the fulfillment of the bar the phone starts ringing on the side of the receiver and then he must press the green button to answer the call. To adjust the volume during a call, you may use the up/down left-side button (2). To close the call press the Red button (3)

6. Receive an encrypted call

When you receive a crypto call, Cryptech automatically gets the call and shows the black Cryptech dialer so that you can recognise it immediately, in case you use the phone also for a normal calls.
Data exchange starts automatically and, at the end of fullfillment of the bar, the phone starts ringing. Normally you will see this phase only if the phone is open, because when it is closed it will ring only when the connection is ready.

7. Define your own cryptographic keys

In a network of encrypted phones (starting from 2) static cryptographic keys are used by the AES256 algorithm to encrypt your conversation. They are often called "*symmetrical*" or "*shared*" because they must be identical for all users or for groups of them.. To create your shared key click:
Menu>(4)settings>
Insert your User Password to access this protected area
Choose (2)phone>(1)CSD crypto call>(3)Key management.
Choose "1 User keys" and create at least one cryptographic key by selecting "New", then typing "1" in the "Priority level" field and a word or a string of characters in the field "Key". **The longer the string you use, the safer will be the key.**
Write down or memorize the word, numbers or string of characters that you insert, because you will have to ask your partners in the network to insert exactly the same string in order to decipher the conversations.
The system will transform the string of characters that you have inserted in an "hash" of 256 characters that will be used by the algorithm to encrypt your conversations The value "1" means "highest priority" and is required to bypass the Cryptech *test* keys. You can see the Test key on the screen, marked "test it is useful when first testing your devices, since you can make encrypted calls even before you decide to create your own keys. Once you have successfully inserted your key/s, you can delete the Cryptech Test key with the "Delete Key" function: click on each key, select "Menu", then "Manage Key" and "Delete Key". **Remember to set the same static shared keys on every device you want to communicate with**

8. Manage your encryption modes

Cryptech supports two types of encryption keys: static (shared) keys and dynamic (based on the Diffie-Hellman protocol). Unlike static keys, the Diffie-Hellman protocol does not require user intervention: if you enable this feature, a dynamic key is created at the beginning of the call and deleted when this is terminated.

Using both static and dynamic keys guarantees maximum security, because your calls will be encrypted with a different key for every conversation. To make sure that the key generated by the Diffie-Hellman protocol is absolutely secure (as there is the remote possibility of an intruder intercepting the key in exact moment of its generation)Cryptech shows two numerical authentication codes that appear on your screen at the beginning of the call. **If you use only Diffie-Hellman you should communicate these codes to each other before starting the conversation**: if they match, no intruder has interfered with the call. Using the combination of static and dynamic keys eliminates all the risks. However several options are available to provide maximum flexibility of usage.

Cryptech by default is configured for highest security, (the combination of static and dynamic keys) . However the Security Levels can be managed selecting: Menu>(4)settings>(2)phone>(1)Csd Crypto call>(2)security option):

Shared Keys
You can select if a shared key can be optional or required

Diffie-Hellman
You can choose if it will be optional, required or disabled
ECDH
By default it is enabled and it means that there will be a generation of a key using Elliptic Curve Diffie Hellman 571 bit Koblitz curve.
If you disable it, Cryptech will use the Diffie-Hellman 4096 bit that is more computationally heavy and considered less strong than ECDH. If one of the phone does not have the ECDH enabled, they will use DH 4096 bit

Select your option according to the set-up of your partners. Whenever possible, we recommend the use all the features enabled.
If you need to communicate with someone that uses "Easy Cryptech" you must set Shared Key "optional" and Diffie-Hellman must not be disabled.

9. Sms key management

Cryptech by default generates automatically a cryptographic key for your SMS. When you make a crypto call to one of your contacts, at the beginning of the connection, Cryptech generates a specific key for that contact and will save it until the next call, when it will change it.
You can see it on the display noticing that a green key will appear on the bottom of the screen. You can choose to create it manually going to: menu>(4)settings>(2)phone>(2)sms crypto>(1)sms key management.
If you want that a crypto SMS is automatically deleted after being received,, decrypted and read, you can set it in::
menu>(4)settings>(2)phone>(2)sms crypto>(2)Flash as default
In this way the message cannot be saved after been read
To send a crypto sms you can go into the menu>(3)smsCrypto>menu>(1)new message or going on to shortcut from the main Cryptech screen pressing the right arrow. Here you will have to write the message , select the receiver from the contacts and send it . If you select automatic key the message will be automatically send encrypted with the key automatically generated and assigned to the contact. If you select to use manual key you will have to insert an encryption key for the message but take care that receiver must know this password to decrypt the message.

10. Encrypted contacts

You can save your Crypto contacts in an encrypted area , where you access only inserting your User Password. You can insert your contacts manually or you can import them from your SIM card going to: Contacts>Menu>(6) Import from SIM
You can import all contacts from the SIM or pressing the Center button to flag those you need and then select the button Import
There is a function that offers you to save the phone number when you receive a call from a number that is not in the contacts list. You can enable it by choosing: menu>(4)settings>(2)phone>(1)CSD crypto Call>(6)Save new contact
Remember that you have two sets of Contacts: one for clear call (if you use them) and one encrypted and protected by User Password for Crypto calls. If you use the clear calls we suggest to import all contacts from SIM in the Clear contacts and to select the few that are in your encrypted network and import them in the Crypto contacts..

11. Audio settings

During the Crypto call you can adjust the volume from 1 to 7(you see the numbers on the display) with the key on the left side of the phone. The normal setting is is 3/4.Take care that if you set the volume at highest level (7) your partner could hear some echo , so we recommend to use this volume level only when in noisy situation.
To adjust the volume of the ringer you have to go into menu>(4)settings>(1)general>(2)ringtone
You can mute the ringer pressing and holding the # button of the keypad and an icon will be displayed on the top of the screen

12. Screen brightness

You can adjust the brightness of the screen by going to: menu>(4)settings>inserting your User Password>(1) General>(5) Brightness. We suggest to use it with the lower luminosity for longer battery duration

13. Lock

You can rapidly lock the phone pressing and holding the * (asterisk) button on the keypad To unlock use the User Password

14. Authentication/time-out

When in Crypto mode, for security reason, the phone will automatically lock itself after not being used for 5 minutes. You can increase or reduce this delay by going to:
menu>(4)settings>(1)general>(1)security>(3)timeout
After this period you will have to authenticate yourself with your User Password.
You can also exclude authentication to make Crypto calls, by going to Menu>4setting>1general>1security>4auth crypto dialer and choosing "disabled" . **We strongly suggest keeping the "enabled" mode so that only yourself can make crypto calls and crypto SMS..**

15. Sim PIN use

You can decide to enable or disable the use of the PIN of your SIM card. If you enable it remember that when you switch on the phone you will have to authenticate yourself twice, first with your SIM PIN and then with your User Password to access to Cryptech Other settings

16. Sim Change notification

If you aware that somebody can stole your phone and substitute the sim card, you can set to be notified if a new sim card insert into the phone. Such a case an sms will be sent to phone number you will set. In the sms will be also insert the gsm cell id the phone is connected to. Having those data you can localize the phone on google map with the use of the KMS . Toset the function select menu>(4)settings>(1)general>(1)security>(5)sim change notify> enable here you have to insert the phone number to be advised of the sim change.

17. Automatic synchronization

Cryptech by default starts synchronization of the call and exchanges keys before ringing on the side of the receiver, in order to avoid him to wait for the process. You can exclude this feature by going to:
Menu>4setting>2phone>1csd crypto call>5 autoanswer. Disabling the auto mode, the phone of the receiver will ring and he will have to answer the call to start synchronization (and wait to speak until it is completed). Take care that with the automatic synchronization if you are in roaming you will be charged for receiving a call also if you didn't press the green button for answer.

18. Change language

Under Menu>(4)setting>(1)general>(5)language you can change the language used by Cryptech .

19. Shortcuts

Form the keypad:
pressing the right arrow of the navigation keypad will start a new message
pressing the up arrow of the navigation keypad will go into the inbox
pressing and holding the * button you lock the phone
pressing and holding the # button you mute the phone

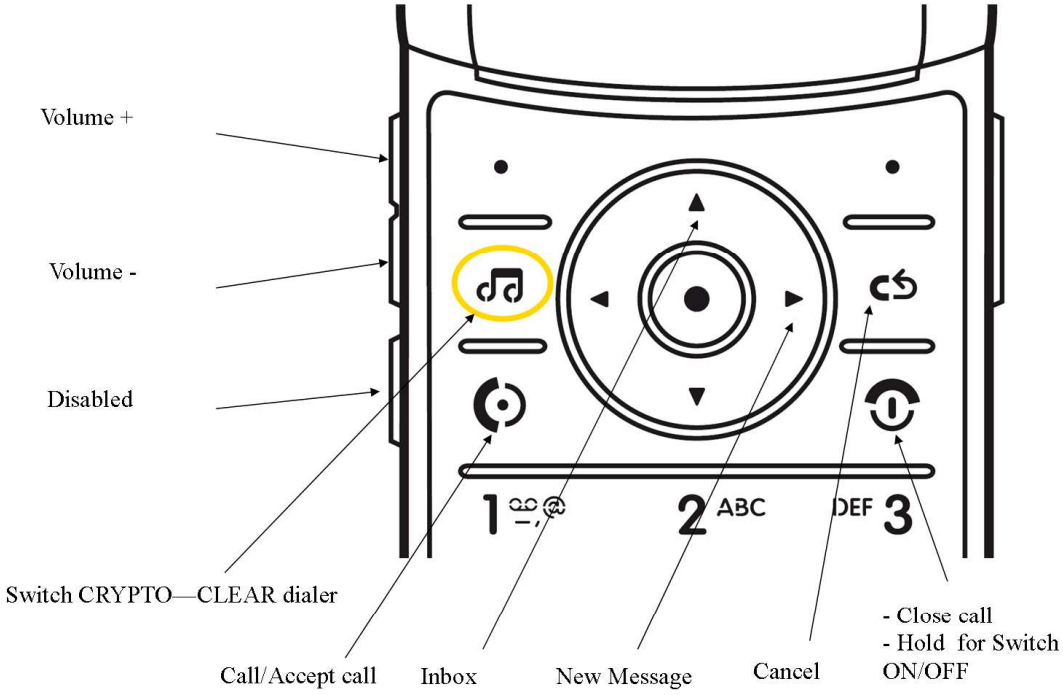
20. Network settings

Press Menu>(4)setting>(2)phone>(1)csd crypto call>(1)network. The Cryptech default network configuration ("v.110" protocol and "*transparent" mode) is optimised for most situations. However in some cases*, for example where the GSM network does not support data roaming or the v.110 protocol, it is advisable to select the "v.32" protocol in the "CSD Line" field.

⚠ **Normally all networks support v.110 and transparent connection if you are in roaming and you are not able to connect to your partner you should try to switch to v.32 and transparent. In some rare cases and very few countries, you must use the DATA number of your partner to make the connection.**

⚠ **Switching between transparent and non transparent can give you a more easy connection during the synchronization but during the crypto call you will notice a little more of delay, particularly if you experience disturbs on the line. On some network you are obliged to use non transparent to be able to call in crypto mode.**

⚠ ***Remember to set v. 110 and transparent when you are back in your country and network***


Volume +
Volume -
Disabled
Switch CRYPTO—CLEAR dialer
Call/Accept call
Inbox
New Message
Cancel
- Close call
- Hold for Switch ON/OFF

Lock phone
Mute phone